(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 January 2001 (11.01.2001)

PCT

(10) International Publication Number
WO 01/03402 A1

(51) International Patent Classification[7]: H04L 29/06, H04Q 7/38

(21) International Application Number: PCT/EP99/04625

(22) International Filing Date: 2 July 1999 (02.07.1999)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA COMMUNICATIONS OY** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **VITIKAINEN, Timo** [FI/FI]; Sinitaiscnpolku 4A3, FIN-02660 Espoo (FI).

(74) Agents: **TRÖSCH, Hans-Ludwig** et al.; Tiedtke-Bühling-Kinne et al., Bavariaring 4, D-80336 München (DE).

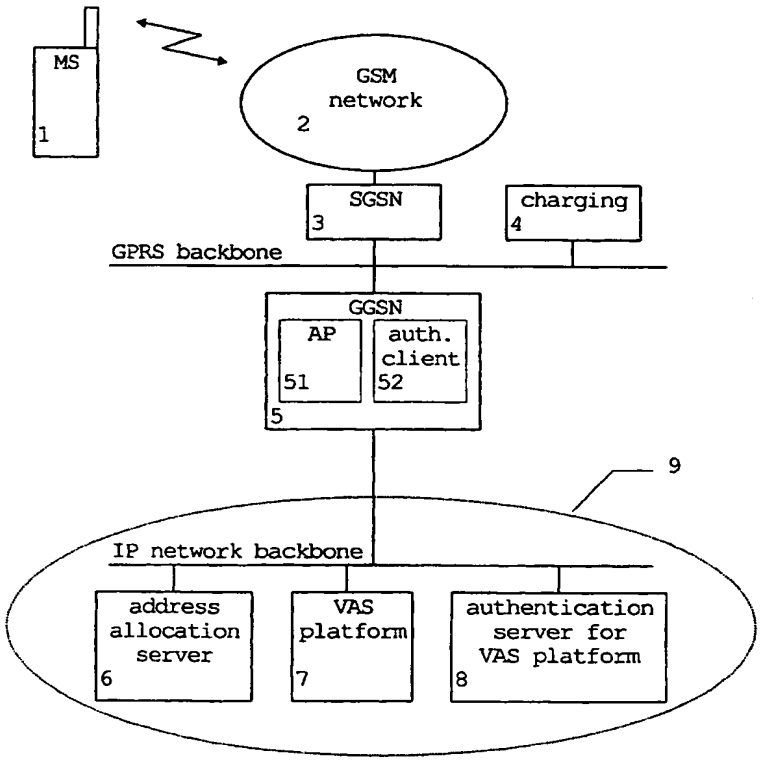
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: AUTHENTICATION METHOD AND SYSTEM



(57) Abstract: The present invention relates to an authentication method and system for identifying a subscriber (1) of a first network (2) in a second network (9), wherein an address of the second network (9) is allocated to the subscriber (1). An information about a mapping between the address of the second network (9) and a subscriber identity is generated and transmitted to the second network (9). Thereby, an authentication server connection is provided between the first network (2) and the second network (9), such that the subscriber identity can be handled over to the second network (9). Thus, a VAS platform of the second network (9) can receive the address of the second network and the subscriber identity of the subscriber (1), such that subscriber accessing services of the VAS platform can be identified for charging and/or addressing purposes.

WO 01/03402 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Authentication method and system

FIELD OF THE INVENTION

The present invention relates to an authentication method and system for identifying a subscriber of a first network in a second network.

BACKGROUND OF THE INVENTION

In a GPRS (General Packet Radio Services) system, a packet mode technique is used to transfer high-speed and low-speed data and signaling in an efficient manner. GPRS optimizes the use of network and radio resources. Applications based on standard data protocols are supported, and interworking is defined with IP-networks. GPRS is designed to support from intermittent and bursty data transfers through to occasional transmission of large volumes of data. Charging is typically based on the amount of data transferred.

GPRS introduces two new network nodes in the GSM mobile network. The Serving GPRS Support Node (SGSN) which is at the same hierarchical level as a mobile switching center (MSC) and which keeps track of the individual location of mobile stations (MS) and performs security functions and access control. The SGSN is connected to the base station system with a Frame Relay. The Gateway GSN (GGSN) provides interworking with external packet-switched networks, and is connected with SGSNs via an IP-based GPRS backbone network. A HLR (Home Location Register) of the GSM system is enhanced with GPRS subscriber information, and a VLR (Visitor Location Register) can be enhanced for more efficient coordination of GPRS and non-GPRS services and functionality, e.g. paging for circuit switched calls that

can be performed more efficiently via the SGSN, and combined GPRS and non-GPRS location updates.

In order to access the GPRS services, an MS first makes its presence known to the network by performing a GPRS attach. This operation establishes a logical link between the MS and SGSN, and makes the MS available for paging via the SGSN, and notification of incoming GPRS data. In order to send and receive GPRS data, the MS shall activate the packet data address it wants to use. This operation makes the MS known in the corresponding GGSN and interworking with external data networks can commence. User data is transferred transparently between the MS and the external data networks with a method known as capsulating and tunneling, wherein data packets are equipped with GPRS-specific protocol information and transferred between the MS and the GGSN. This transparent transfer method lessens the requirement for the GPRS mobile network to interpret external data protocols, and it enables easy introduction of additional interworking protocols in the future.

In case a mobile subscriber wishes to access a value added service (VAS) provided by an IP network, a service specific charging is a mandatory feature of the corresponding VAS platform for mobile operators. This means that operators need service platforms which are capable of performing charging based on e.g. an accessed WML content or URL (Uniform Resource Locator) and delivered messages. However, MS identification in VAS platforms connected to the GPRS network or other mobile packet switched networks is not trivial. The reason therefore is that a VAS platform receives only IP packets from a certain source address which is normally only a dynamic IP address of an MS and thus not sufficient at all for identifying that MS.

Furthermore, an MSISDN (Mobile Station ISDN number) is required which is especially important for messaging services (e.g. multimedia messaging) in order to prevent additional HLR queries.

A known MS identification is performed e.g. by using user names, passwords or cryptographic keys. However, these types of solutions are complex to operate/manage for mobile operators. Moreover, such solutions normally require their own management systems and data bases which are not necessarily consistent with existing billing or charging systems of mobile operators where the IMSI (International Mobile Subscriber Identity) or the MSIDSN are the key of the CDRs (Call Detail Records).

Alternatively, an authentication service could be performed in the HLR. However, this solution leads to a significant rise of the load in the HLR which is already a crucial node.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide an authentication method and system, by means of which VAS platforms may identify an MS accessing services of the VAS platform.

This object is achieved by an authentication method for identifying a subscriber of a first network in a second network, comprising the steps of:
allocating an address of said second network to said subscriber;

generating information about a mapping between the subscriber's address in said second network and a subscriber identity; and
transmitting the mapping to said second network..

Furthermore, the above object is achieved by Authentication system for identifying a subscriber of a first network in a second network, comprising:
a gateway device comprising allocation means for allocating an address of said second network to said subscriber, and authentication client means for generating an information about a mapping between said address of said second network and a subscriber identity, and for transmitting said mapping information to said second network; and
an authentication server provided in said second network and adapted to log and maintain said mapping information.

Furthermore, the above object is achieved by a gateway device for connecting a first network to a second network, comprising:
allocation means for allocating an address of said second network to a subscriber of said first network; and
authentication client means for generating an information about a mapping between said address of said second network and a subscriber identity, and for transmitting said mapping information to said IP network.

Accordingly, a mapping information between the address of the second network and the subscriber identity is generated and supplied to the second network. Thereby, a client-server connection is achieved, which allows the actual subscriber identity of a dynamic address of the second network to be handled over to the second network. The

second network uses the mapping of the address of the second network and the subscriber identity for identifying the subscriber.

Since the first network, e.g. the GGSN, includes an information about the mapping between the address of the second network and the subscriber identity, new mapping data can be transmitted to the second network, if the mapping has changed.

Preferably, the subscriber identity is the IMSI and/or the MSISDN of the subscriber. Thereby, a multimedia messaging service may identify the recipient using the MSISDN, and the recipient may identify the message sender based on the MSISDN provided by the multimedia messaging service center, such that HLR queries are no longer required. Furthermore, the MSISDN or IMSI may be used by a charging function for identifying the subscriber in order to perform a service specific charging.

The mapping information may be transmitted in an access request message, such as a RADIUS access request message.

Preferably, an authentication server functionality may be provided for a VAS platform, wherein the access request message is transmitted to the authentication server functionality of the VAS platform, and the mobile terminal is identified in the VAS platform based on the mapping information. In this case, the authentication server functionality may be included in the VAS platform or, alternatively, the authentication server functionality may be provided by a dedicated authentication server.

In case the gateway device is a GGSN, the mapping information may be generated by an authentication client functionality in the GGSN.

The mapping information may be used for a service specific charging.

The authentication server may be a RADIUS server for the VAS platform provided in the second network, wherein the VAS platform is adapted to identify the subscriber based on the mapping information.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, the present invention will be described in greater detail on the basis of a preferred embodiment with reference to the accompanying drawings, in which:

Fig. 1 shows a block diagram of a GPRS network connected to an IP network according to the preferred embodiment of the present invention, and

Fig. 2 shows an information flow and processing diagram of an access operation to the IP network, according to the preferred embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

In the following, the preferred embodiment of the authentication method and system according to the present invention will be described on the basis of a GPRS network which is an example for a first network and an IP network which is an example for a second network.

According to Fig. 1, a mobile terminal or mobile station (MS) 1 is radio-connected to a GSM network 2 which in turn is connected to an SGSN 3 of a GPRS backbone network. The GPRS backbone network includes a charging server 4 and a GGSN 5 connected to an IP network 9, e.g. an intranet of a specific operator or the Internet.

The GGSN 5 comprises an access point unit (AP) 51 which provides an access to the IP network 9 and which is arranged to allocate an IP address to an MS to be connected to the IP network 9. Furthermore, the GGSN 5 includes an authentication client unit 52 adapted to provide required parameters for an access request issued to the IP network 9. Moreover, the authentication client unit 52 may be arranged to clarify/specify the handling of user name and password parameters supplied to the desired VAS of the IP network 9.

According to an example of the preferred embodiment shown in Fig. 1, the IP network 9 is an operator's intranet backbone which comprises an address allocation server 6, e.g. a RADIUS (Remote Authentication Dial In User Service) server, a DHCP (Dynamic Host Configuration Protocol) server or a DNS (Domain Name Server), or the like. The address allocation server 6 is arranged to respond to an access request from the GGSN 5 with either an access-accept or an access-reject message. Furthermore, the address allocation server 6 performs a host configuration and address allocation in the IP network 9.

Additionally, the IP network 9, e.g. the operator's intranet, comprises a Value Added Service (VAS) platform 7. An example for such a VAS platform may be a Multimedia

Messaging Center (MMSC) for delivering multimedia messages to requesting subscribers such as the MS 1. Moreover, another example for a VAS platform is a Wireless Application Protocol (WAP) gateway which provides an access to the World Wide Web (WWW) based on a corresponding Uniform Resource Locator (URL).

According to the preferred embodiment of the present invention, a dedicated authentication server 8 for the VAS platform 7 is provided in the IP network 9. The authentication server 8 may be a RADIUS server which accepts or rejects access requests to the VAS platform 7. Furthermore, the authentication server 8 is arranged to log or store an access request or a corresponding mobile subscriber identity, received from the authentication client, e.g. RADIUS client, 52 of the GGSN 5. Accordingly, the authentication client 52 of the GGSN 5 communicates with the address allocation server or specific authentication server 8, such that an authentication client-server connection is established.

In particular, the authentication client 52 incorporates or adds a mapping information to the access request, based on which the actual MSISDN and/or IMSI of an MS requesting a service from the IP network 9 can be derived at the authentication server 8. The mapping information may comprise the current IP address, the MSISDN and/or the IMSI, or any combination or shortened version, based on which the MSISDN and/or IMSI can be derived from the current IP address. The MSISDN can be obtained by the GGSN 5 via the SGSN 3 from GSM network 2.

Thus, the authentication client unit 52 of the GGSN 5 provides an information about the mapping between the IP

address and the MSISDN and/or the IMSI. If this mapping is changed, the authentication client unit 52 sends a new mapping information to the authentication server 8 of the IP network 9. Thereby, the MSISDN and/or IMSI is always available to the VAS platform 7.

The MSISDN can be provided as an additional GTP parameter supplied from the SGSN 3 to the GGSN 5. The IMSI can be derived from the TID also supplied from the SGSN 3 to the GGSN 5.

The GGSN 5 functions as an access point of the GSM GPRS data network for interworking with the IP network 9. In this case, the GPRS network will look like any other IP network or subnetwork. The access to the IP network 9 may involve specific functions such as user authentication, users authorization, end-to-end encryption between an MS and the IP network 9, allocation of a dynamic IP address belonging to the addressing space of the IP network 9. In case of a non-transparent access to the IP network 9, the GGSN 5 takes part in the functions listed above. In particular, the MS 1 requesting access to the IP network 9 is given an address belonging to the operator addressing space. The address is given either at subscription, in which case it is a static address, or at PDP (Packet Data Protocol) context activation, in which case it is a dynamic address. This address is used for packet forwarding between the IP network 9 and the GGSN 5 and within the GGSN 5.

In the following, an example for an access operation to the IP network 9 via the GPRS backbone network is described based on Fig. 2.

Fig. 2 shows an information flow and processing diagram indicating the signaling and processing actions performed during the exemplary access operation. According to Fig. 2, the MS 1 sends an Activate PDP Context Request message to the SGSN 3, including protocol configuration options and parameters such as an NSAPI (Network layer Service Access Point Identifier). Then, the SGSN 3 creates a TID for the requested PDP context by combining the IMSI stored in the MM (Mobility Management) context with the MSAPI received from the MS, wherein the SGSN fetches the MSISDN from the HLR. Subsequently, the SGSN 3 transmits a Create PDP Context Request message to the GGSN 5 including parameters such as an APN (Access Point Name), the TID and the MSISDN. The AP unit 51 of the GGSN 5 allocates an IP address for the MS 1, and the authentication client unit 52 incorporates required parameters for the access request to the authentication server 8. In particular, the authentication client unit 52 generates mapping data indicating a mapping between the allocated IP address and the MSISDN/IMSI.

The GGSN 5 sends the access request including the IP address and the mapping data to the authentication server 8 provided for the VAS platform 7. Then, the authentication server 8 accepts or rejects the received request. Furthermore, the authentication server 8 logs the request including the IP address and the mapping data. Accordingly, the VAS platform 7 is capable of identifying the MS 1 based on the mapping data included in the access request stored in the authentication server 8.

The GGSN 5 sends back to the SGSN 3 a Create PDP Context Response message, wherein a cause value is set according to the result of the authentication, i.e. access rejected or

accepted. Depending on the cause value received in the Create PDP Context Response message, the SGSN 3 sends either an Activate PDP Context Accept message or an Activate PDP Context Reject message to the MS 1.

Accordingly, by the above access procedure, the VAS platform 7 can receive the IP address, the IMSI and the MSISDN of an accessing MS, such that the addressing in the multimedia messaging service can be based on the MSISDN and service specific charging is possible.

In summary, the present invention relates to an authentication method and system for identifying a subscriber of a first network in a second network, wherein an address of the second network is allocated to the subscriber. An information about a mapping between the address of the second network and a subscriber identity is generated and transmitted to the second network. Thereby, an authentication server connection is provided between the first network and the second network, such that the subscriber identity can be handled over to the second network. Thus, a VAS platform of the second network can receive the address of the second network and the subscriber identity of the subscriber, such that subscriber accessing services of the VAS platform can be identified for charging and/or addressing purposes.

It is to be noted that the above described authentication method and system can be applied between any gateway device between two networks, such as a mobile network and an IP network, or a telephone network (e.g., ISDN, PSTN) and a closed or open data network. Moreover, the authentication server 8 and authentication client unit 52 are not

restricted to a RADIUS server and client. It is also to be noted that multiple VAS platforms, similar to or different from each other, can be attached to the second network at the same time.

The above description of the preferred embodiment and the accompanying drawings are only intended to illustrate the present invention. The preferred embodiment of the invention may thus vary within the scope of the attaches claims.

Claims

1. An authentication method for identifying a subscriber of a first network **(2)** in a second network, comprising the steps of:

a) allocating an address of said second network **(9)** to said subscriber;

b) generating information about a mapping between the subscriber's address in said second network **(9)** and a subscriber identity; and

c) transmitting the mapping to said second network.

2. An authentication method according to claim 1, wherein said mapping information is transmitted to said second network, when said mapping between said address in said second network and the subscriber identity has changed.

3. An authentication method according to claim 1 or 2, wherein said subscriber identity is an IMSI and/or an MSISDN of the subscriber.

4. An authentication method according to any one of claims 1 to 3, wherein said mapping information is transmitted in an access request message.

5. An authentication method according to claim 4, wherein said request access message is a RADIUS access request message.

6. An authentication method according to claim 4 or 5, further comprising the steps of providing an authentication

server functionality for a VAS platform, transmitting said access request message to said authentication server functionality, and identifying said subscriber in the VAS platform based on said mapping information.

7. An authentication method according to claim 6, wherein said authentication server functionality is included in the VAS platform.

8. An authentication method according to claim 6, wherein said authentication server functionality is provided by a dedicated authentication server.

9. An authentication method according to any one of the preceding claims, wherein said mapping information is generated by an authentication client functionality in a GGSN.

10. An authentication method according to any one of the preceding claims, wherein said mapping information is used for a service specific charging and/or addressing of mobile terminals.

11. An Authentication system for identifying a subscriber **(1)** of a first network **(2)** in a second network **(9)**, comprising:

a) a gateway device **(5)** comprising allocation means **(51)** for allocating an address of said second network **(9)** to said subscriber **(1)**, and authentication client means **(52)** for generating an information about a mapping between said address of said second network **(9)** and a subscriber identity, and for transmitting said mapping information to said second network **(9)**; and

b) an authentication server **(8)** provided in said second network **(9)** and adapted to log and maintain said mapping information.

12. An authentication system according to claim 11, wherein said gateway device is a GGSN **(5)**.

13. An authentication system according to claim 11 or 12, wherein said authentication client means **(52)** is a RADIUS client.

14. An authentication system according to any one of claims 11 to 13, wherein said authentication server **(8)** is a RADIUS server for a VAS platform **(7)** provided in said second network **(9)**, wherein said VAS platform **(7)** is adapted to identify said subscriber **(1)** based on said mapping information.

15. An authentication system according to any one of claims 11 to 14, wherein said subscriber identity is an IMSI or an MSISDN.

16. An authentication system according to any one of claims 11 to 15, wherein said authentication client means **(52)** is arranged to transmit said mapping information in an access request message to said authentication server **(8)**.

17. A gateway device for connecting a first network **(2)** to a second network **(9)**, comprising:

a) allocation means **(51)** for allocating an address of said second network **(9)** to a subscriber **(1)** of said first network **(2)**; and

b) authentication client means **(52)** for generating an information about a mapping between said address of said second network **(9)** and a subscriber identity, and for transmitting said mapping information to said IP network **(9)**.

18. A gateway device according to claim 17, wherein said authentication client means **(52)** is arranged to transmit said mapping information in an access request message.

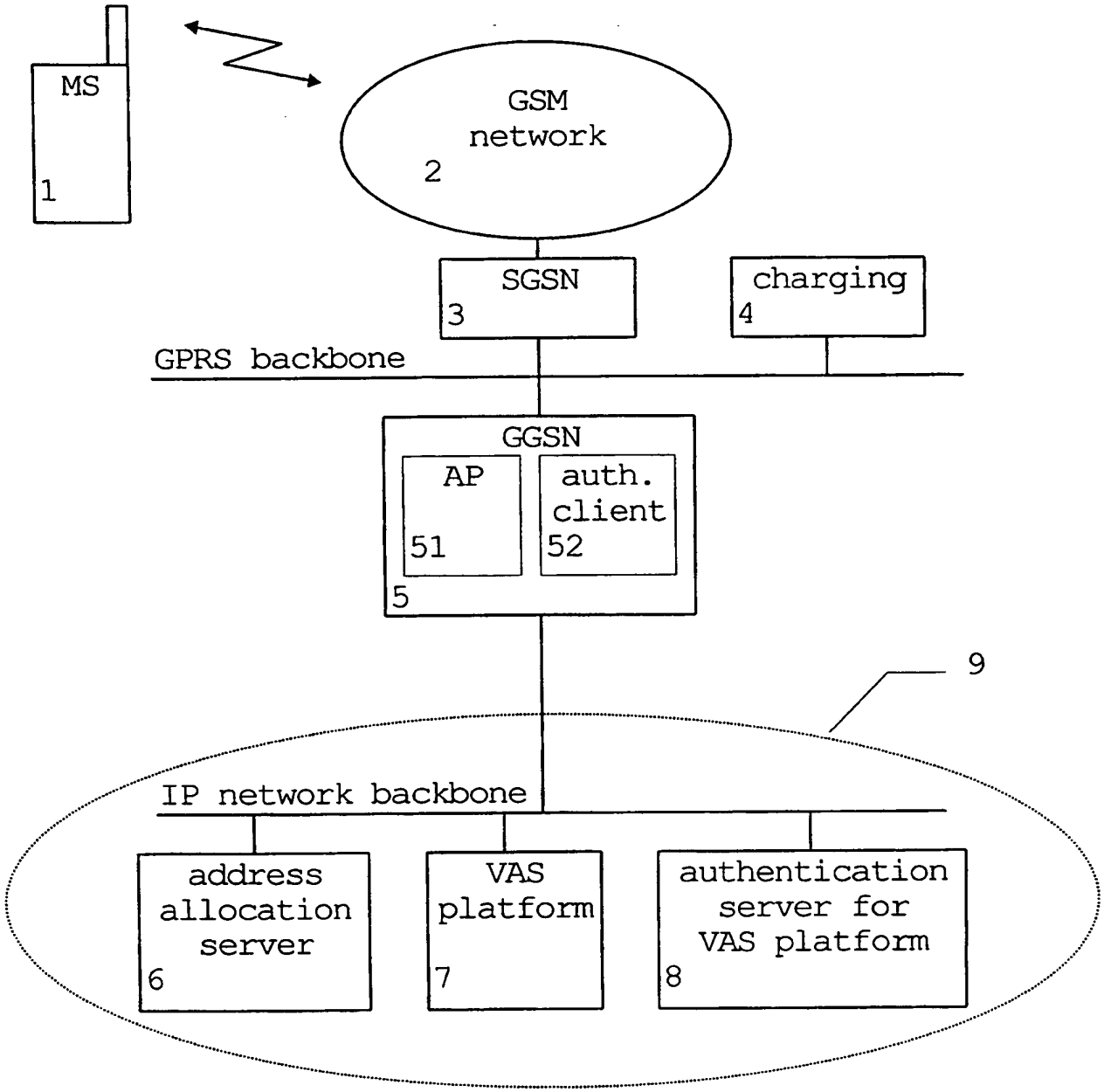

MS
1
GSM
network
2
SGSN
3
charging
4
GPRS backbone
GGSN
AP
51
auth.
client
52
5
9
IP network backbone
address
allocation
server
6
VAS
platform
7
authentication
server for
VAS platform
8

Fig. 1

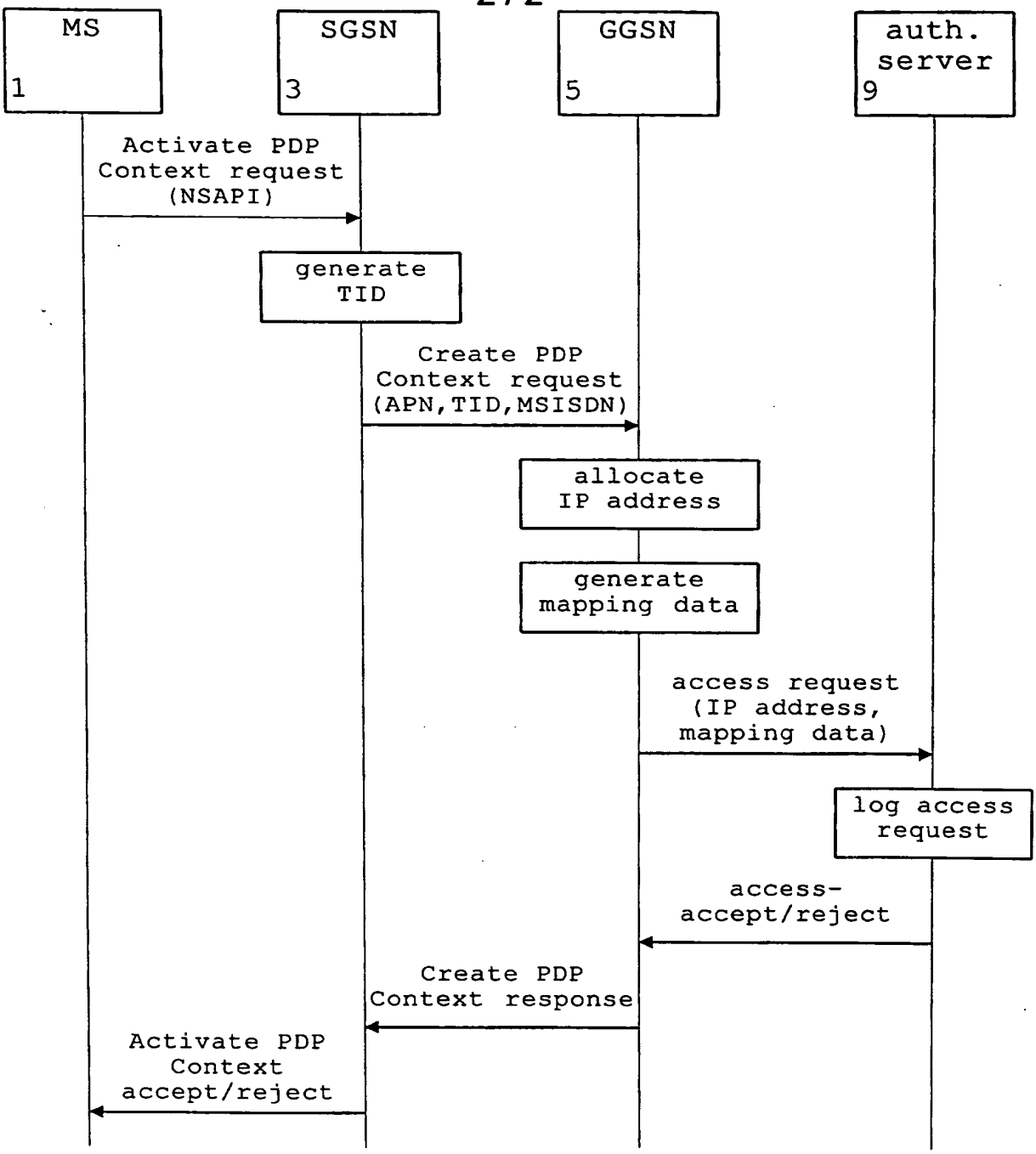

MS
1
SGSN
3
GGSN
5
auth. server
9
Activate PDP Context request (NSAPI)
generate TID
Create PDP Context request (APN,TID,MSISDN)
allocate IP address
generate mapping data
access request (IP address, mapping data)
log access request
access-accept/reject
Create PDP Context response
Activate PDP Context accept/reject

Fig. 2

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/EP 99/04625

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2 280 085 A (VODAFONE LTD) 18 January 1995 (1995-01-18) abstract page 2, line 1 - line 20 page 3, line 5 -page 4, line 11 page 11, line 12 -page 12, line 21	1-18
A	WO 95 32592 A (REININGHAUS GEORG ;SIEMENS AG (DE)) 30 November 1995 (1995-11-30) abstract page 3, line 4 - line 33 page 7, line 5 - line 17 page 7, line 34 -page 8, line 18	1-18

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 May 2000	18/05/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Adkhis, F

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. tional Application No
PCT/EP 99/04625

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2280085 A	18-01-1995	AU 6978494 A	17-01-1995
		WO 9501069 A	05-01-1995
WO 9532592 A	30-11-1995	DE 4417779 C	07-12-1995
		CN 1152990 A	25-06-1997
		EP 0760192 A	05-03-1997
		JP 2971948 B	08-11-1999
		JP 9508772 T	02-09-1997
		US 5898922 A	27-04-1999